⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－182758

⑤1Int.Cl.⁴	識別記号	庁内整理番号	④3公開　昭和63年(1988)7月28日
G 06 F 12/14	320	B－7737－5B	
9/06	330	A－7361－5B	
G 09 C 1/00		7368－5B	審査請求　未請求　発明の数 1　(全4頁)

⑤4発明の名称　情報記憶装置

⑳特　願　昭62－14903
㉒出　願　昭62(1987)1月23日

⑦2発明者　中莖　洋一郎　東京都港区芝5丁目33番1号　日本電気株式会社内
⑦1出願人　日本電気株式会社　東京都港区芝5丁目33番1号
⑦4代理人　弁理士　内原　晋

明　細　書

発明の名称　情報記憶装置

特許請求の範囲

外部より入力されるキーを格納する手段と、装置固有の内部キーを記憶する手段と、情報を記憶する記憶手段と、外部より入力されるデータを前記外部キー及び内部キーを用いて暗号化して前記記憶手段に格納すると共に、前記記憶手段より読み出された情報を前記外部、内部キーを用いて復号する暗号処理部とから構成される情報記憶装置。

発明の詳細な説明

（産業上の利用分野）

本発明は暗号化方式を用いた情報記憶装置である。

（従来の技術）

記憶媒体上のデータの守秘、記憶されたプログラム等の複製使用の防止の方法として、次のような方法が知られている。データの守秘に関しては、元のデータを暗号化してから媒体上に格納する方法が知られており、これは暗号化のためのキーを用いて暗号化及び復号を行う方法である。また一方、プログラム等を複写して複数の装置上で使用されることを防止するための方法として知られているのは、媒体に特殊なフォーマットを施したり、セクタ長を変える等の特別な記録の方式を採用する方法である。

（発明が解決しようとする問題点）

まず、暗号化によるデータ守秘法においては、暗証番号等のキーの値さえ分かれば暗号文を平文に復号することができるという危険性を持っている。本発明の第一の目的はこのようなキーの盗難等に対する安全性を高めることである。

また、記憶媒体にプログラム等を特殊な形式で記録して複写を防止した場合、それを読み出すためのプログラム等を解析することにより記録の形式が解明されてしまう恐れがある。また、この場合バックアップ用の媒体を作成することも妨げて

しまうために、媒体の内容が破壊された場合には復旧が不可能となる欠点があった。本発明の第二の目的は、媒体上のプログラム等の複写を行うことは妨げず、且つそれらの複写された媒体が複数の装置上で同時に利用されることを防ぐことにある。

（問題点を解決するための手段）

外部より入力されるキーを格納する手段と、装置固有の内部キーを記憶する手段と、情報を記憶する記憶手段と、外部より入力されるデータを前記外部キー及び内部キーを用いて暗号化して前記記憶手段に格納すると共に、前記記憶手段より読み出された情報を前記外部、内部キーを用いて復号する暗号処理部とから構成される情報記憶装置。

（作用）

本装置を用いて記憶媒体上に記録した情報を正しく読み出すためには、その情報の書きこみ時に使用した装置に固有のキーとその時に外部から設定したキーの両方が必要となる。このために外部から設定したキーのみでは記録内容を正しく読み込むことを極めて困難にすることが可能となる。また、媒体への記録は通常の形式で行うことができるために記録された内容を別の媒体へ複写することは容易に可能であるが、上記の理由により書き込みに用いた装置でのみ正しく復号された情報の読み出しが可能であるため、本装置で記録されたプログラム等を複製しても複数の装置上で同時に使用することは不可能である。

（実施例）

次に第1図から第4図を参照して本発明の実施例について説明する。

第1図は一実施例の概要を示したもので、外部から設定されたキーは外部キー保持部1に記録される。また、装置固有のキーは内部キー記憶部2に保持されている。これらのキーを組み合わせて、暗号処理部3で入力データ4の暗号化及び、記憶装置上の暗号化データ6の復号を行う。外部キー、内部キーの組み合わせ方としては、四則演算、ビット毎の論理演算等を用いて新たなキーを生成し、そのキーで実際の暗号化・復号を行う方法や、一方のキーで暗号化した後に他方のキーでさらにもう一度暗号化する方法等が挙げられる。

ここで、書き込み時に使用した内部キー・外部キーとそれぞれ全く同じ内部キー・外部キーの組み合わせを用いた時のみ正しく元の情報が得られるような暗号化の方式を採用し、またそれと同時に後に述べるような方法等で、装置内部に保持している内部キーを直接外部から読み取られないように工夫することによって、書き込み時に使用した装置なしでは正しく記録内容を読み取る事を事実上不可能にすることができる。

第2図の例は第1図で示したような装置を情報守秘に応用した例である。内部キー記憶部8を暗号処理装置本体から取り外し可能とすることで、書き込み時に使用した内部キーを独立に管理することを可能としている。従って万一、外部キーの値を知られてしまったとしても、この場合には内部キーを用いずには記録内容を読み出すことは殆ど不可能であるためにより安全に情報を記録しておくことが可能である。また、第3図の様に記憶媒体9としてフロッピーディスク等の持ち運びが容易な媒体を用いた場合には、書き込み時に使用した内部キー記憶部8と記録媒体9が揃って初めて内容を読み出すことが可能であるため、媒体の輸送等を行う場合の安全性をより高くすることが可能である。

第4図はプログラム等の複製使用防止に利用した例で、上例と同様に書き込み時に使用した内部キー記憶装置8を持った装置でのみ記録内容の正しい読み出しが可能となる。従って記録媒体9と内部キー記憶部8が一体となって初めて使用可能となるため、後に述べるような方法等によって内部キーの値の読み出しを禁止することで内部キー記憶部8の複製を防止することが出来る。従って、媒体の方を多数複製してもそれらが同時に読み出し使用されることを防ぐことが可能となる。

実際に内部キーの値の読み出しを防ぐ方法としては次のようなものが考えられる。例えば本装置を1個のＬＳＩとして実現し、内部キーはその中

のメモリ部に書き込む方法をとるもので、ＬＳＩの機能として、その内部キーの書き込み機能を持たせ、読み取り機能は持たせないことにより外部からの内部キー値の読みだしを防ぐことができる。あるいは一般のＰＲＯＭ等を利用して内部キーを格納する場合には、ＬＳＩの端子・配線等を完全に絶縁する等の方法で、外部からの読みだしを不可能にすることが可能である。

（発明の効果）

従来、外部から入力されるキーの値のみによって暗号化を行っていたのに対して、本発明では各装置に固有の内部キーと組み合わせて実際の暗号化を行うため、万一外部キーの値を知ることが出来ても実際に暗号化された文を正しく読み出すためには、事実上計算不可能であるような膨大な計算量を必要とさせることが可能であるため、より高い安全性を確保することが可能となった。

また、媒体に記録されたデータの複写は許すかわりに装置内部に保持されたキーの複製を防ぐことにより、データやプログラムのバックアップを可能としつつも複製使用を防止することが可能となった。

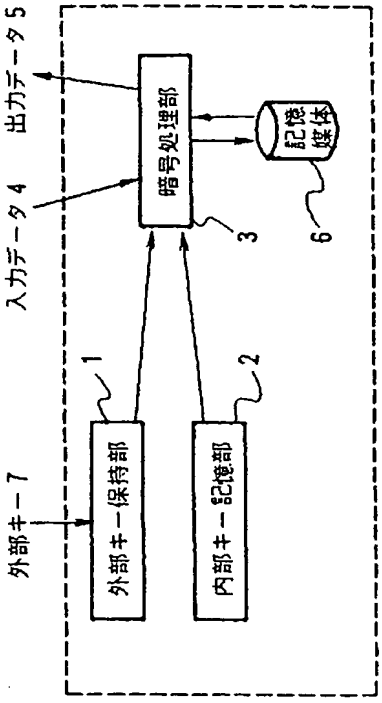
図面の簡単な説明

第１図は本装置の基本的な構成を示す図で、第２図は情報守秘に応用した場合の構成図、第３図は外部記憶媒体を対象とした場合の構成図、第４図は外部記憶媒体上のプログラムの複製使用防止に応用した場合の構成図である。

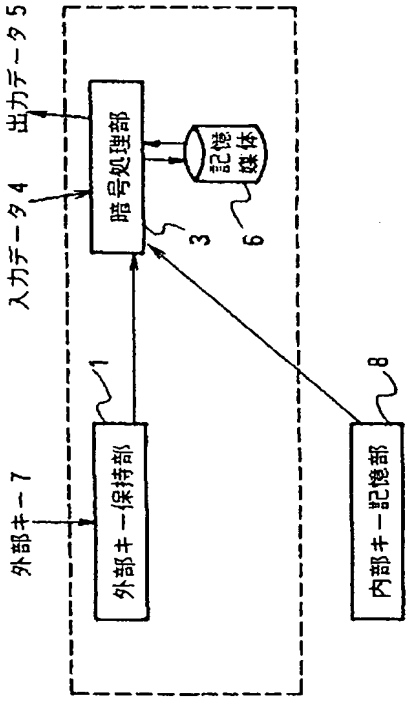
図において、１は外部キー保持部、２は内部キー記憶部、３は暗号処理部、４は入力データ、５は出力データ、６は記憶媒体、７は外部キー、８は取り外し可能とした内部キー記憶部、９は取り外しが可能な記憶媒体。

代理人　弁理士　内原　晋

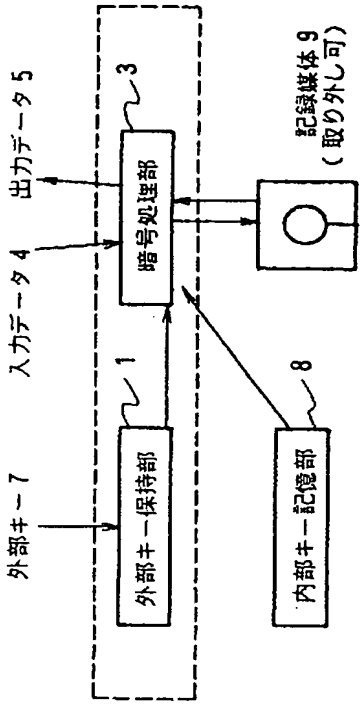
第１図



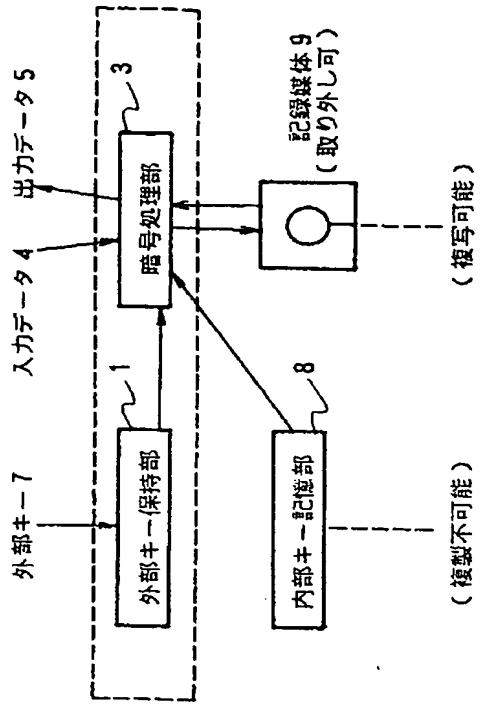
第２図



第 3 図


外部キー7
入力データ4
出力データ5
外部キー保持部
1
暗号処理部
3
内部キー記憶部
8
記録媒体9
(取り外し可)

第 4 図


外部キー7
入力データ4
出力データ5
外部キー保持部
1
暗号処理部
3
内部キー記憶部
8
記録媒体9
(取り外し可)
(複写可能)
(複製不可能)